ABSTRACT

A secure digital content delivery system includes a content provider and a content user. The content provider delivers encrypted content to the content user in response to delivery requests. The content provider generates encryption algorithms on the fly and encrypts the content prior to delivery, using a different encryption algorithm and key for each content delivery. The content user subsequently requests access permission from the content provider, to access the encrypted content. The content provider grants access by generating an executable decryption module on the fly and providing the executable decryption module to the content user. The content user decrypts the content and accesses it on the fly, using the executable decryption module. The accessed content is then re-encrypted using a different encryption algorithm and key, to preserve the integrity of the secure content delivery system. The content delivery system uses a programmably configurable protocol parsing engine to encrypt and decrypt content.